CLAIM AMENDMENTS

1. (Currently Amended) A method of securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, the method comprising the computer-implemented steps of:

receiving non-encrypted authentication request information that includes challenge information from the first node;

receiving, from an authentication server that is separate from but communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information and including challenge response information generated by the authentication server; and

establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

2. (Original) A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

3. (Currently Amended) A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

4. (Currently Amended) A method as recited in Claim 1, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:

determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and

issuing a request for authentication to the authentication server only when the authentication request information was created within the ~~acceptable~~ specified interval of time with respect to the current time.

5. (Previously Presented) A method as recited in Claim 1, further comprising the steps of:
receiving a password that is associated with the first node;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information; and
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

6. (Previously Presented) A method as recited in Claim 1, further comprising the steps of:
receiving a password that is associated with the first node;
generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information based on CHAP; and
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

7. (Currently Amended) A method of securely establishing a call in a voice over Internet Protocol call connection system that includes a first gateway at a call origination point, a first gatekeeper, a second gatekeeper, a second gateway at a call termination point, and an authentication server that is separate from but communicatively coupled to the first gatekeeper and the second gatekeeper, the method comprising the computer-implemented steps of:
receiving non-encrypted authentication request information from the first gateway;

receiving from the authentication server an authentication message that includes challenge response information generated by the authentication server and indicating whether the first gateway is authenticated based on the non-encrypted authentication request information that includes challenge information; and

establishing a call between the second gateway and the first gateway only when the authentication message indicates that the first gateway is authenticated at the authentication server.

8. (Previously Presented) A method as recited in Claim 7, further comprising the steps of:

receiving a call setup request message at the first gateway;

creating and storing the non-encrypted authentication request information based on the current time and information that uniquely identifies the first gateway; and

requesting the second gateway to set up a call based on the authentication request information.

9. (Currently Amended) A method as recited in Claim 8, further comprising the steps of:

determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; at the second gatekeeper; and

requesting the authentication server to carry out authentication of the first gateway only when the authentication request information was created within the ~~acceptable~~ specified interval of time with respect to the current time at the second gatekeeper.

10. (Original) A method as recited in Claim 7, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

11. (Currently Amended) A method as recited in Claim 7, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

12. (Previously Presented) A method as recited in Claim 7, further comprising the steps of:
receiving a password that is associated with the first gateway;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information; and
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

13. (Currently Amended) ~~The~~ A method as recited in Claim 7, further comprising the steps of:
receiving a password that is associated with the first gateway;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information;
issuing authentication approval information in the authentication message to the second gatekeeper only when the authentication response matches the authentication request information; and
issuing authentication rejection information in the authentication message to the second gatekeeper when the authentication response does not match the authentication request information.

14. (Previously Presented) A method as recited in Claim 7, further comprising the steps of:
receiving a password that is associated with the first gateway;

generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information based on CHAP; and

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

15. (Previously Presented) A method as recited in Claim 12, wherein the step of establishing a call between the second gateway and the first gateway comprises the step of establishing a call between the second gateway and the first gateway only when authentication approval information is received in the authentication message.

16. (Currently Amended) A method of securely establishing a call in a voice over Internet Protocol call connection system that includes a first gateway at a call origination point, a first gatekeeper, a second gatekeeper, a second gateway at a call termination point, and an authentication server that is separate from but communicatively coupled to the first gatekeeper and the second gatekeeper, the method comprising the computer-implemented steps of:

receiving user identification information from the first gateway that comprises a user identifier and a personal identification number that are uniquely associated with a calling party who originates a call using the first gateway;

receiving from the authentication server a first authentication message indicating whether the user identification information is authenticated based on first challenge response information generated by the authentication server;

receiving non-encrypted authentication request information that includes challenge information from the first gateway;

receiving from the authentication server a second authentication message indicating whether the first gateway is authenticated based on the non-encrypted authentication request information and second challenge response information generated by the authentication server; and

establishing a call between the second gateway and the first gateway for the calling party only when the first authentication message indicates that the user identification information is authenticated and the second authentication message indicates that the first gateway is authenticated at the authentication server.

17. (Original) A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

18. (Currently Amended) A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

19. (Currently Amended) A method as recited in Claim 16, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:

determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and

issuing a request for authentication to the authentication server only when the authentication request information was created the ~~acceptable~~ specified interval of time with respect to the current time.

20. (Previously Presented) A method as recited in Claim 16, further comprising the steps of:

receiving a password that is associated with the first gateway;

generating an authentication response based on the password and challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information; and

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

21. (Previously Presented) A method as recited in Claim 16, further comprising the steps of:

receiving a password that is associated with the first gateway;

generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information based on CHAP; and

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

22. (Currently Amended) A method as recited in Claim 16, wherein the step of receiving non-encrypted user identification information further comprises the steps of:

determining whether the user identification information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and

issuing a request for authentication to the authentication server only when the user identification information was created within the ~~acceptable~~ specified interval of time with respect to the current time.

23. (Previously Presented) A method as recited in Claim 16, further comprising the steps of:

retrieving a personal identification value that is associated with the user account number in the user identification information;

determining whether the personal identification value matches the personal identification number that is in the user identification information; and

issuing authentication approval information in the authentication message only when the personal identification value matches the personal identification number that is in the user identification information.

24. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:
receiving non-encrypted authentication request information that includes challenge information from the first node;
receiving, from an authentication server that is separate from but communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information and challenge response information generated by the authentication server; and
establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

25. (Original) A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

26. (Currently Amended) A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

27. (Currently Amended) A computer-readable medium as recited in Claim 24, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:

determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and

issuing a request for authentication to the authentication server only when the authentication request information was created within the ~~acceptable~~ specified interval of time with respect to the current time.

28. (Previously Presented) A computer-readable medium as recited in Claim 24, further comprising the steps of:

receiving a password that is associated with the first node;

generating an authentication response based on the password and challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information;

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

29. (Previously Presented) A computer-readable medium as recited in Claim 24, further comprising the steps of:

receiving a password that is associated with the first node;

generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;

determining whether the authentication response matches the authentication request information based on CHAP; and

issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

30. (Currently Amended) An apparatus for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, which instructions, comprising:

means for receiving non-encrypted authentication request information that includes challenge information from the first node;

means for receiving, from an authentication server that is separate from but communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information and challenge response information generated by the authentication server; and

means for establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

31. (Currently Amended) An apparatus for securely establishing a call between a first node of a voice over Internet Protocol call connection and a second node thereof, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving non-encrypted authentication request information that includes challenge information from the first node;

receiving, from an authentication server that is separate from but communicatively coupled to the second node, an authentication message indicating whether the first node is authenticated based on the non-encrypted authentication request information and challenge response information generated by the authentication server; and

establishing a call between the second node and the first node only when the authentication message indicates that the first node is authenticated at the authentication server.

32. (Previously Presented) An apparatus as recited in Claim 30, wherein the means for receiving non-encrypted authentication request information comprises means for receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

33. (Currently Amended) An apparatus as recited in Claim 30, wherein the means for receiving non-encrypted authentication request information comprises means for receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

34. (Currently Amended) An apparatus as recited in Claim 30, wherein the means for receiving non-encrypted authentication request information further comprises:
means for determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and
means for issuing a request for authentication to the authentication server only when the authentication request information was created within the ~~acceptable~~ specified interval of time with respect to the current time.

35. (Previously Presented) An apparatus as recited in Claim 30, further comprising:
means for receiving a password that is associated with the first node;
means for generating an authentication response based on the password and challenge information contained in the authentication request information;
means for determining whether the authentication response matches the authentication request information; and
means for issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

36. (Previously Presented) An apparatus as recited in Claim 30, further comprising:
means for receiving a password that is associated with the first node;
means for generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;
means for determining whether the authentication response matches the authentication request information based on CHAP; and
means for issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.

37. (Previously Presented) An apparatus as recited in Claim 31, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving an access token comprising a general identifier value, a time stamp value, a challenge value, and a random value.

38. (Currently Amended) An apparatus as recited in Claim 31, wherein the step of receiving non-encrypted authentication request information comprises the steps of receiving ~~an H.235 ClearToken~~ data comprising a general identifier value, a time stamp value, a challenge value, and a random value.

39. (Currently Amended) An apparatus as recited in Claim 31, wherein the step of receiving non-encrypted authentication request information further comprises the steps of:
determining whether the authentication request information was created within ~~an acceptable~~ a specified interval of time with respect to a current time; and
issuing a request for authentication to the authentication server only when the authentication request information was created within the ~~acceptable~~ specified interval of time with respect to the current time.

40. (Previously Presented) An apparatus as recited in Claim 31, further comprising one or more sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving a password that is associated with the first node;
generating an authentication response based on the password and challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information; and
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information.

41. (Previously Presented) An apparatus as recited in Claim 31, further comprising one or more sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:
receiving a password that is associated with the first node;
generating a Challenge Handshake Authentication Protocol (CHAP) response based on the password and implied CHAP challenge information contained in the authentication request information;
determining whether the authentication response matches the authentication request information based on CHAP; and
issuing authentication approval information in the authentication message only when the authentication response matches the authentication request information based on CHAP.